UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,073	12/10/2003	Hugh S. Njemanze	25137-11332	8491

758 7590 03/19/2007

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/733,073	NJEMANZE, HUGH S.	
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/10/2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :05/08/2006, 06/26/2006 and 01/29/2007.

DETAILED ACTION

1. Claims 1-24 are pending in this application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 5-11, 13-18 and 20-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (Patent No.: US 6,704,874 B1), hereinafter Porras in view of Berthaud et al. (Patent No.: US 6,157,957).

4. As to claim 1, Porras discloses a network security system (abstract) comprising: a first distributed software agent to collect a first stream of alerts from a first network security device having a first clock (FIG. 1, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock (column 6, lines 13-17); a second distributed software agent to collect a second stream of alerts from a second network security device having a second clock (FIG. 1, items 12-16 referred to different networks, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the second stream representing an event detected by the second network security

device and including a time of detection by the second network security device according to the second clock (column 6, lines 13-17); and a manager module in communication with the distributed software agents to receive the first and second stream of alerts (FIG. 1, column 3, lines 62-67 and column 4, lines 10-26), identify a common event represented by a first alert in the first stream from the first network security device and by a second alert in the second stream from the second network security device (column 6, lines 19-27 and column 8, lines 37-47).

Porras doesn't explicitly disclose synchronizing first clock and second clock using common event. However, Berthaud discloses synchronizing first close and second clock using common event (FIG. 2, column 9, lines 35-60).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras by synchronizing first close and second clock using common event as taught by Berthaud in order to "regularly compute parameters necessary for elaborating a continuous conversion function." (Berthaud)

5. As to claim 9, Porras discloses a method performed by a network security system, the method (abstract) comprising: receiving a first stream of alerts from a first network security device having a first clock (FIG. 1, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock (column 6, lines 13-17);

receiving a second stream of alerts from a second network security device having a second clock (FIG. 1, items 12-16 referred to different networks, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock (column 6, lines 13-17); identifying a common event represented by a first alert in the first stream from the first network security device and by a second alert in the second stream from the second network security device (FIG. 1, column 3, lines 62-67 and column 4, lines 10-26; column 6, lines 19-27 and column 8, lines 37-47).

Porras doesn't explicitly disclose synchronizing first clock and second clock using common event. However, Berthaud discloses synchronizing first close and second clock using common event (FIG. 2, column 9, lines 35-60).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras by synchronizing first close and second clock using common event as taught by Berthaud in order to "regularly compute parameters necessary for elaborating a continuous conversion function." (Berthaud)

6. As to claim 16, Porras discloses a machine readable medium storing a set of instructions that, when executed by the machine (FIG. 1), cause the machine to: receive a first stream of alerts from a first network security device having a first clock (FIG. 1, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in

the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock (column 6, lines 13-17); receive a second stream of alerts from a second network security device having a second clock (FIG. 1, items 12-16 referred to different networks, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock (column 6, lines 13-17); identify a common event represented by a first alert in the first stream from the first network security device and by a second alert in the second stream from the second network security device (FIG. 1, column 3, lines 62-67 and column 4, lines 10-26; column 6, lines 19-27 and column 8, lines 37-47).

Porras doesn't explicitly disclose synchronizing first clock and second clock using common event. However, Berthaud discloses synchronizing first close and second clock using common event (FIG. 2, column 9, lines 35-60).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras by synchronizing first close and second clock using common event as taught by Berthaud in order to "regularly compute parameters necessary for elaborating a continuous conversion function." (Berthaud)

7. As to claims 2, 10 and 17, Porras discloses the network security system wherein the manager module determines a synchronization error using the time of detection of the common event in the first alert and the time of detection of the common event in the second alert (column 6, lines 18-27 and column 8, lines 37-51).

Porras doesn't explicitly disclose synchronizing the first clock and the second clock and correcting the synchronization error based on common event. However, Berthaud discloses synchronizing first clock and second clock and correcting synchronization error using common event (FIG. 2, column 9, lines 35-60).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras by synchronizing the first clock and the second clock and correcting the synchronization error based on common event as taught by Berthaud in order to "regularly compute parameters necessary for elaborating a continuous conversion function." (Berthaud)

8. As to claims 3, 11 and 18, Porras doesn't explicitly disclose synchronizing the first clock and the second clock by selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock. However, Berthaud discloses synchronizing the first clock and the second clock by selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock (column 2, lines 42-61).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras by synchronizing the

first clock and the second clock by selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock as taught by Berthaud in order to provide accurate converted time values with a pre-determined precision.

9. As to claims 5, 13 and 20, Porras doesn't explicitly disclose synchronizing the first clock and the second clock by adjusting a time offset associated with the first clock. However, Berthaud discloses synchronizing the first clock and the second clock by adjusting a time offset associated with the first clock (column 3, lines 1-5; column 5, lines 15-67 and column 6, lines 1-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras by synchronizing the first clock and the second clock by adjusting a time offset associated with the first clock as taught by Berthaud in order to "regularly compute parameters necessary for elaborating a continuous conversion function." (Berthaud)

10. As to claims 6, 14 and 21, Porras discloses the network security system wherein the manager module identifies a common event by detecting a new Internet Protocol (IP) address in the first alert and the second alert (column 6, lines 13-17).

11. As to claims 7, 15 and 22, Porras discloses the network security system wherein the manager module identifies a common event by determining that the second alert is corroborative of the first alert (column 6, lines 13-27 and column 8, lines 37-51).

12. As to claim 8, Porras discloses the network security system wherein the first network security device comprises an Intrusion Detection System (IDS) (column 2, lines 18-38).

13. As to claim 23, Porras discloses a network security system (abstract) comprising: a plurality of distributed software agents to each collect alerts from a plurality of corresponding network security devices (FIG. 1, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17); and a manager module in communication with the distributed software agents to receive the alerts (column 3, lines 62-67 and column 4, lines 10-26), identify a common event represented by alerts from a subset of the plurality of network security devices (column 6, lines 19-27 and column 8, lines 37-47).

Porras doesn't explicitly disclose synchronizing the subset of network security devices using the common event. However, Berthaud discloses synchronizing the subset of network security devices using the common event.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras by synchronizing the subset of network security devices using the common event as taught by Berthaud in

order to "regularly compute parameters necessary for elaborating a continuous conversion function." (Berthaud)

14. As to claim 24, Porras doesn't explicitly disclose synchronizing the subset of network security devices by adjusting timestamps in each alert received from the subset of network security devices. However, Berthaud discloses synchronizing the subset of network security devices by adjusting timestamps in each alert received from the subset of network security devices (column 3, lines 1-5; column 5, lines 15-67 and column 6, lines 1-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras by synchronizing the subset of network security devices by adjusting timestamps in each alert received from the subset of network security devices as taught by Berthaud in order to "regularly compute parameters necessary for elaborating a continuous conversion function." (Berthaud)

15. Claims 4, 12 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras in view of Berthaud and further in view of Apel et al. (Patent No.: US 6,760,687 B2), hereinafter Apel.

16. As to claims 4, 12 and 19, neither Porras nor Berthaud explicitly discloses wherein selecting one of the first and second clocks comprises determining a

relationship of the first and second clocks to a system-wide reference clock. However, Apel disclose wherein selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock (column 9, lines 8-15 and lines 60-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras and Berthaud by selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock as taught by Apel in order to "provide a highly accurate and flexible system" (Apel)

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

Liou et al. (Pub No.: US 2002/0136335 A1) discloses method for synchronizing clock in distributed systems.

Turaki (Patent No.: US 5402394) discloses method for synchronizing clock based on common time base by selecting a reference clock.

Hein (Patent No.: US 6,148,049) discloses a method for synchronizing clock based on evaluating a value and a time of received timemark data.

Connary et al. (Pub. NO.: US 2004/0044912 A1) discloses determing threat level associated with network activity.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100